DATA CATEGORIZATION

Practice 4.2.2

Issue Date: 09/27/2006
Effective Date: 09/27/2006

1. Purpose

   Owners of information systems must appropriately categorize data to assure expected outcomes. Data categorization consists of two aspects, availability and confidentiality. Categorization ultimately drives system design incorporating appropriate redundancy of key components and needed levels of security.

2. Revision History

Revision Date	Revision Number	Change Made	Reviser
08/03/2007	01	Updated format to match with ISF V2.0 and standard policy documentation	C. Bradley
07/20/2010	02	Changes resulting from annual review	T. Stahl

3. Persons, Groups, Systems Affected

   All agencies within the Executive Branch of Indiana State Government excluding separately elected

4. Responsibilities

   4.1. System Owner - individuals responsible for all aspects of the system must assure their data is categorized appropriately and the ISI is current and complete.

   4.2. Indiana Office of Technology – responsible for maintenance of the database.

5. Procedures

   1. Appendix 1 contains a decision tree designed to assist agencies determine the Availability requirements of their data/system. This information should be entered into the Information Systems (ISI) found at http://isi.iot.in.gov/.

   2. Appendix 2 contains a decision tree aimed at assisting agency determinations of their data/system Confidentiality rating. This information should be entered into the Information Systems (ISI) found at http://isi.iot.in.gov/.

   3. The ISI should be updated as changes impact the system. Examples requiring an update to the ISI include changes to business owners, Availability categorization, and Confidentiality categorization.

6. Compliance

Availability Data Categorization will be used to determine disaster recovery efforts and plan for needed infrastructure. A failure to maintain the information can risk agency's systems being included in disaster recovery planning. IOT security will periodically review data to ensure completeness and communicate with agencies to ensure new systems have been added.

Confidentiality rating will be the agency's responsibility to maintain. The rating and a system risk assessment will result in a security plans that result in appropriate protective measures.

7. Definitions/References

Availability

There are three Availability categories:

Critical – systems agencies deem too important to be down for more than 6 hours and where budgeted funds cover the costs required limit downtime to this period of time.
Necessary – systems that cannot be down for more than 7 days and where budgeted funds cover the costs required to limit downtime to this period of time.
Non-critical – systems with no firm expectation set regarding duration restored on a best efforts basis.

Note – The definitions above consider worst case scenarios requiring the State's secondary data center for processing. This timeframe is not indicative of the expected downtime impacts for routine hardware and software system problems. Service Level Agreements better set expectations for ordinary problems.

Confidentiality

There are four Confidentiality categories:

Confidential – systems holding the most sensitive information intended strictly for use within the State or State agency. This information is exempt from disclosure under the provisions of the Freedom of Information Act, HIPAA, or other applicable federal laws or regulations. Its unauthorized disclosure could seriously and adversely impact the State, the State agency, its business partners, its customers, or individual persons. Examples of confidential information include: Health care, law enforcement, and taxpayer personal and financial information.
Sensitive – systems holding information requiring special precautions to assure the integrity of the information and protection from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness. Examples of sensitive information include financial transactions and regulatory actions.
Private – systems holding personal information intended for use within the State or State agency. Its unauthorized disclosure could seriously and adversely impact the State or State agency and/or its employees.
Public – systems holding other information not clearly fitting into any of the above three classifications. Disclosure, in some cases may be limited by policy, but disclosure doe not negatively impact the State or State agency, its employees, and/or its customers. Public information falls in one of two areas:

1. Public-Controlled: Information is Public but accuracy must be maintained and access must be controlled by specific procedures. Example: BMV driver's records.
2. Public-Published: Accuracy is not critical and the information is freely published or posted. Example: Agency telephone listings.

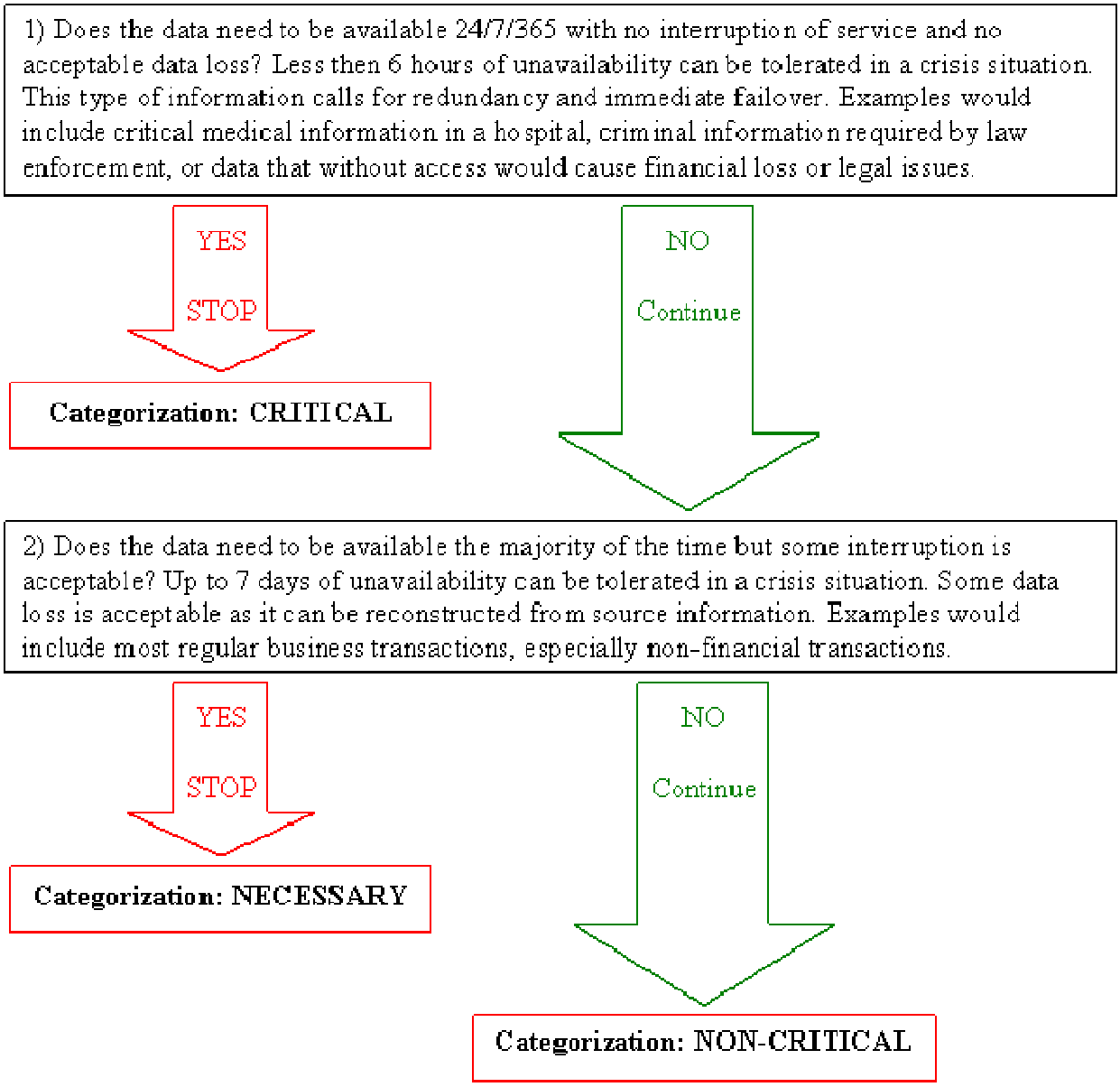
8. Appendices

Appendix 1 – Availability Decision Tree
Appendix 2 – Confidentiality of Data Decision Tree

Appendix 1

Availability Decision Tree

The following questions are designed to assist in determining the minimum Availability category for the data you maintain. You may assign a higher level to the data at your discretion. **Please note that the integrity of the data must be maintained regardless of the category assigned.**



Appendix 2

Confidentiality of Data Decision Tree

The following questions are designed to assist in determining the minimum Confidentiality category for the data you maintain. You may assign a higher level to the data at your discretion. **Please note that the integrity of the data must be maintained regardless of the category assigned.** Aggregates of data should be classified as to the most secure classification level (e.g. when data of mixed classification exist in the same database, file, report, etc., the classification of that database, file, or report should be that of the highest level of classification).